UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,167	12/05/2003	Thomas A. Crispin	CNTR.2224-C1	2865

23669 7590 12/13/2007

HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
12/13/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	Application No.	Applicant(s)	
	10/730,167	CRISPIN ET AL.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27,56-64 and 66-83* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27,56-64 and 66-83* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :4/11/07, 5/2/07, 5/23/07 (x2), 5/24/07 (x3), 5/31/07 (x3), 6/22/07, and 9/11/07. *b* 10/19/07

DETAILED ACTION

1. Claims 1-27, 56-64, and 66-83 remain for examination. The correspondence filed 8/4/07 amended claims 1-27, 56, and 67.

2. Because the Applicant did not adequately traverse the declaration of Official Notice from the previous Office Action (see page 9, at #13), these declarations are now taken as admissions of prior art, as per MPEP 2144.03(c).

Information Disclosure Statement

3. The information disclosure statements (IDS) submitted on 4/11/07, 5/2/07, 5/23/07, 5/24/07, 5/31/07, 6/22/07, and 9/11/07 have all been considered by the Examiner. Additionally, Examiner has included an updated copy of the relevant portion of the IDS of 7/25/06 indicating that the previously objected reference CN1431584A has since been considered. Examiner would also like to respectfully suggest that in the future, Applicant may wish to expedite the examination process by refraining from submitting redundant IDS forms all listing the same reference (see the five IDS submissions of 5/23 and 5/24) as well as consolidating multiple references to be considered onto one IDS form (see the multiple IDS forms, all filed 5/31/07, each listing different references).

Specification

4. The amendment(s) to the specification and the abstract are acknowledged. Examiner has determined that they do not add new matter, and are thus acceptable.

Response to Arguments

5. Applicant's arguments filed 8/4/07 have been fully considered but they are not persuasive. Beginning on page 19 of the amendment of 8/4/07, Applicant primarily argues that the instant invention differs from the prior art in that the prior art discloses the use of a cryptographic co-processor, rather than a microprocessor, to execute the recited instruction; however, this is an artificial distinction as the co-processor is itself a microprocessor (see the enclosed dictionary reference), and furthermore there is nothing in the claims that would preclude the claimed microprocessor from being utilized as a co-processor in a more complex computer system. With respect to the new limitations of claims 1 and 56, it is first observed that the ability of a microprocessor to fetch an instruction flow (i.e. a computer program) from memory has been inherent to microprocessors in general since well nigh time immemorial (see the Von Neumann Architecture reference). Nevertheless, Kessler explicitly discloses wherein the co-processor is capable of retrieving an instruction flow (i.e. a macro security operation comprising a plurality of primitive security operations: col. 4, lines 10-16 & Figure 7) from a memory queue (further imparting the proper order, or flow, of execution of said instructions, col. 5, lines 8-17), and wherein each of the primitive instructions being executed has the opcode and prefix field as identified from the previous Office Action.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1-6, 11, 23-27, 56-60, and 77-83 are rejected under 35 U.S.C. 102(e) as being anticipated by Kessler et al (U.S. Patent 6,789,147).

Regarding claims 1 and 56:

Kessler discloses a (microprocessor) apparatus for performing cryptographic operations comprising: fetch logic, configured to fetch an instruction flow from memory for execution by a microprocessor (col. 4, line 59 – col. 5, line 36), said instruction flow comprising an instruction, configured to direct said microprocessor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 – col. 6, line 10).

Regarding claims 2 and 83:

Kessler further discloses wherein the cryptographic operations are accomplished at the level of system privileges afforded to application programs (SSL being a component of web browser applications: col. 4, lines 5-10).

Regarding claims 3 and 57:

Kessler further discloses an encryption operation encrypting a plurality of blocks of input data to generate a plurality of ciphertext blocks (e.g. col. 2, lines 13-14 etc.)

Regarding claims 4 and 58:

Kessler further discloses an decryption operation decrypting a plurality of blocks of input data to generate a plurality of plaintext blocks (Ibid).

Regarding claims 5 and 59:

Kessler further discloses using AES (col. 9, lines 13-15; element 807 of Figure 8)

Regarding claims 6 and 60:

Kessler further discloses a block cipher mode to be employed in accomplishing the cryptographic operations (inherent to the block ciphers taught in col. 9, lines 10-20).

Regarding claim 11:

Kessler further discloses wherein the instruction proscribes that the cryptographic operations be accomplished on a plurality of text blocks (Figure 7)

Regarding claims 23 and 78:

Kessler further discloses a cryptography unit, configured to receive a plurality of said associated micro instructions, and configured to execute a plurality of cryptographic

rounds on each of said plurality of blocks of input data to generate each of a plurality of output text blocks, wherein said plurality of output text blocks are prescribed by said control word (Figure 8; col. 9, lines 7-55).

Regarding claims 24 and 79:

Kessler further discloses block cipher logic, configured to perform a plurality of cryptographic rounds on each of said plurality of blocks of input data according to said one of the block cryptographic operations to produce said corresponding plurality of output text blocks (col. 9, lines 7-44); and key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to a plurality of cryptographic rounds, and configured to provide each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds (col. 9, lines 23-55).

Regarding claims 25 and 80:

Kessler further discloses wherein said block cipher logic id divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more of said plurality of blocks of data (inherent to at least the AES and 3DES algorithms disclosed on col. 9, lines 10-20).

Regarding claims 26 and 81:

Kessler further discloses an integer unit, coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operations (arithmetic unit: col. 9, lines 15-20).

Regarding claims 27 and 82:

Kessler further discloses wherein said opcode field directs said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds (col. 5, lines 40-50).

Regarding claim 77:

Kessler further discloses translation logic, configured to translate said cryptographic instructions into associated micro instructions that specify sub operations required to accomplish said cryptographic operation (e.g. col. 8, lines 11-16).

Claim Rejections - 35 USC § 103

8. Claims 7-10 and 61-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler as applied to claims 6 and 60 above, and further in view of the "Applied Cryptography, 2nd Edition" (hereinafter, "Schneier"; submitted by Applicant in the IDS forms filed 9/25/05 and 3/11/06).

Regarding claims 7-10 and 61-64:

Although Kessler discloses using block cipher modes for at least some of the supported encryption algorithms, it does not explicitly mention any of the modes listed in these claims. However, Schneier teaches that each mode (ECB, CBC, CFB, and OFB) were well known in the art (pages 193-206); accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use any of these modes in the cryptographic processor disclosed by Kessler; each mode has its own particular advantages as disclosed by Schneier (page 209, as appropriate).

9. Claims 12 and 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler.

Regarding claims 12 and 66:

It is now taken as Applicant-admitted prior art[1] that the instruction set of the cryptographic apparatus disclosed by Kessler would be prescribed according to the x86 instruction format, in order to facilitate its use with a common x86 host processor.

10. Claims 13-22 and 67-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler as applied to claims 1 and 56 above, and further in view of Johns-Vano et al. (U.S. Patent 6,026,490)

---

[1] Applicant's traversal of the rejections of claims 12 and 66 (see the amendment of 8/4/07, page 21, 1st paragraph) is inadequate, insofar as the traversal was limited to asserting that the claims should be allowable by merit of Applicant's belief that the parent claims 1 and 56 should also be allowable.

Regarding claims 13 and 67:

Although Kessler discloses at least one register (element 220 of Figure 2), it does not explicitly state that the instruction implicitly references a plurality of registers in the device. However, Johns-Vano discloses that the instruction set of a cryptographic processor implicitly references a plurality of internal registers (elements 558, 560, 564, 552, 566, and 556 of Figure 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made for a cryptographic processor to employ a plurality of registers. One would do so because using hardware registers would be conducive to making a cryptographic processing engine suitable for manufacture in semiconductor foundries thereby reducing manufacturing costs (col. 2, lines 28-33).

Regarding claims 14 and 68:

Johns-Vano further discloses a first register, wherein contents of said first register comprise a pointer to a first memory address, said first memory address specifying a first location in said memory for access of a plurality of input text blocks upon which the cryptographic operations is to be accomplished (col. 5, lines 1-55).

Regarding claims 15 and 69:

Johns-Vano further discloses a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding

plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing the cryptographic operations upon a plurality of input text blocks (col. 5, lines 1-55).

Regarding claims 16 and 70:

Johns-Vano further discloses a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks (col. 5, lines 1-55).

Regarding claims 17 and 71:

Johns-Vano further discloses a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access to cryptographic key data for use in accomplishing the cryptographic operations (col. 5, lines 1-55).

Regarding claims 18 and 72:

Kessler and Johns-Vano further disclose wherein said cryptographic key data comprises a cryptographic key (Kessler: col. 6, lines 40-50; Johns-Vano: col. 7: 1-5).

Regarding claims 19 and 73:

Kessler further discloses wherein said cryptographic key data comprises a cryptographic key schedule (inherent to the algorithms used in col. 9, lines 10-20).

Regarding claims 20 and 74:

Johns-Vano further discloses a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing the cryptographic operations (col. 5, lines 1-55).

Regarding claims 21 and 75:

Johns-Vano further discloses a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of said control word for use in accomplishing the cryptographic operations, wherein said control word prescribes cryptographic parameters for cryptographic operations (col. 5, lines 1-55).

Regarding claims 22 and 76:

Kessler further discloses an encryption/decryption field, configured to prescribe whether the cryptographic operation is an encryption operation or a decryption operation (col. 5, lines 50-60).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Definition of "coprocessor" from the American Heritage Dictionary, as provided by the dictionary.com website, establishing that coprocessors are microprocessors
- PC Mechanic: Von Neumann Architecture establishes that fetch logic for instruction flows had been inherent to computers by the time of the invention

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
10/1/07

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100